DX User IP II

User Guide

w w w . m i n i c o m . c o m

International HQ

Jerusalem, Israel

Tel: + 972 2 535 9666

minicom@minicom.com

North America

Linden, NJ, USA

Tel: + 1 908 486 2100

info.usa@minicom.com

Technical support - support@minicom.com

SC_5UM60000 V1.2 2/09

Table of Contents

1. Welcome 3
2. Introduction 4
2.1 Standalone mode or KVM.net 5
2.1.1 Standalone mode 5
2.1.2 KVM.net enabled / managed 5
3. Features of DX User IP II 5
4. DX User IP II components 6
4.1 Cables 6
5. DX User IP II front panel 6
5.1 DX User IP II rear panel 7
6. Rack mounting the DX User IP II 8
7. Pre-installation guidelines 8
8. Connecting the DX User IP II 8
8.1 Connecting the DX User IP to the WAN/LAN 9
8.2 Connecting the DX User IP II to the DX Central unit 9
8.3 Local User 9
8.4 Serial cable - KVM.net managed mode only 9
8.5 Connecting an RS232 terminal 10
8.5.1 Order of powering on 10
9. Configuring the system – web interface 10
9.1 Initial settings - Default IP address 10
9.2 Static IP addresses for a number of units 11
9.3 Logging into the Web interface 11
9.4 SSL Certificate notes 12
10. Network > Configuration 12
10.1 LAN 1 13
10.2 KVM.net 13
11. Administration > User Settings 14
11.1 Adding a user 15
11.2 Editing a user 15
11.3 Deleting a user 15
11.4 Blocking a user 15
12. Administration > Switch Configuration 16
13. Administration > Serial Settings 17
13.1 Show 17
13.2 Assign to RPS 17
14. Security > Settings 18

15. Security > SSL Certificate 19
16. Maintenance > Firmware Upgrade 19
17. Restore Factory Settings 20
18. Troubleshooting - Safe mode 20
18.1 Entering Safe mode 21
18.2 Restoring factory defaults 22
18.3 Restoring the device firmware 22
19. Saving changes 23
20. Configuring the DX AIM 23
20.1 Standalone and KVM.net Enabled modes - DX AIM configuration 25
20.2 KVM.net managed mode - DX AIM configuration 25
20.2.1 Accessing AIM when the DX system is KVM.net managed 27
21. Configuring the KVM.net 27
21.1 Connecting more than one DXU IP II to the system 31
22. Operating the system 32
22.1 Accessing servers/devices via the IP toolbar 32
22.1.1 The IP Toolbar 32
22.1.2 Accessing a server/device 33
22.2 Taking over a busy remote session 34
22.3 Full screen mode 35
22.4 Changing the performance settings 35
22.5 Adjusting the Video settings 36
22.5.1 Refresh 36
22.5.2 Manual Video Adjust 37
22.5.3 Auto Video Adjust 38
22.6 Power cycle 38
22.7 Keyboard key sequences 38
22.8 Synchronizing mouse pointers 40
22.8.1 Aligning the mouse pointers 40
22.8.2 Calibrating mouse pointers 40
22.8.3 Manual mice synchronization 41
22.9 Minicom logo menu features 43
22.10 Disconnecting the remote session 44
22.11 Accessing servers/devices via KVM.net 44
23. Video resolution and refresh rates 45
24. Technical specifications 46
25. Safety 47
26. User Guide feedback 47
27. WEEE compliance 47

1. Welcome

Thank you for buying the DX User IP II system. The DX User IP II system is produced by Minicom Advanced Systems Limited.

Technical precautions

This equipment generates radio frequency energy and if not installed in accordance with the manufacturer's instructions, may cause radio frequency interference.

This equipment complies with Part 15, Subpart J of the FCC rules for a Class A computing device. This equipment also complies with the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications. These above rules are designed to provide reasonable protection against such interference when operating the equipment in a commercial environment. If operation of this equipment in a residential area causes radio frequency interference, the user, and not Minicom Advanced Systems Limited, will be responsible.

Changes or modifications made to this equipment not expressly approved by Minicom Advanced Systems Limited could void the user's authority to operate the equipment.

Minicom Advanced Systems Limited assumes no responsibility for any errors that appear in this document. Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Minicom Advanced Systems Limited.

© 2007 Minicom Advanced Systems Limited. All rights reserved.

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

2. Introduction

The DX User IP II from Minicom Advanced Systems features remote KVM access and control via a LAN or Internet connection. DX User IP II provides a non-intrusive solution for remote access and control. Remote access and control software runs on the DX User IP II embedded processors only and not on the servers, so there is no interference with server operation or impact on network performance.

Using one or several DX User IP II units with the DX Central allows access to multiple remote servers. The DX User IP II combines digital remote KVM access via IP networks with a comprehensive and integrated system management.

Figure 1 illustrates the basic configuration of the DX system with the DX User IP II and DX Users connected to peripheral devices via the DX Central.

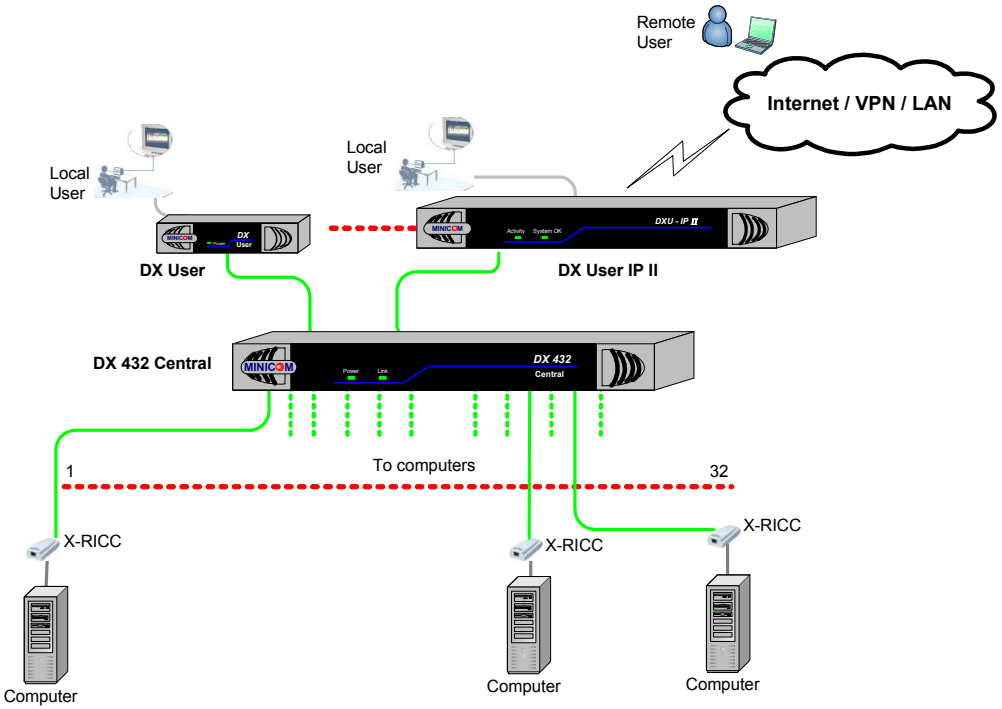

Figure 1 DX User IP II usage scenario

2.1 Standalone mode or KVM.net

DX User IP II can be used in any of the following 3 modes:

- Standalone
- KVM.net enabled
- KVM.net managed

KVM.net is a centralized IP based system for secure control of servers and network devices, power and user administration in the data center environment. KVM.net combines Out-Of-Band, KVM via IP access with modern IT standards and requirements. It is the most comprehensive remote server maintenance solution available in the market today.

These 3 modes are now explained.

2.1.1 Standalone mode

Standalone mode refers to using the DX User IP II as part of the DX system only and working via the DX AIM interface without KVM.net, for remote KVM access and control via a LAN or Internet connection.

2.1.2 KVM.net enabled / managed

The DX User IP II can be KVM.net enabled or KVM.net managed. Both of these refer to managing and accessing servers connected to the DX system via the KVM.net Manager.

KVM.net enabled means the DX is still capable of working in Standalone mode. KVM.net managed means the DX is fully managed and controlled by KVM.net, access to the AIM interface is blocked but can be achieved where necessary via hotkeys. Details of the differences between KVM.net enabled and managed will be explained in the configuration and operating sections later on in this Guide.

3. Features of DX User IP II

- KVM (keyboard, video, mouse) access over IP
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Connect a user console for direct access to KVM switch (In Standalone or KVM.net enabled mode)

DX User IP II supports PS/2 type keyboards and mice and HD 15 video output.

4. DX User IP II components

The DX User IP II package consists of:

- DX User IP II
- Cables
- Brackets to rack mount the DX User IP II
- Supplied CD

4.1 Cables

The DX User IP II package contains the following cables.

- CAT5 FTP cable (2M/6Ft)
- Serial cable

5. DX User IP II front panel

Figure 2 illustrates the DX User IP II front panel.

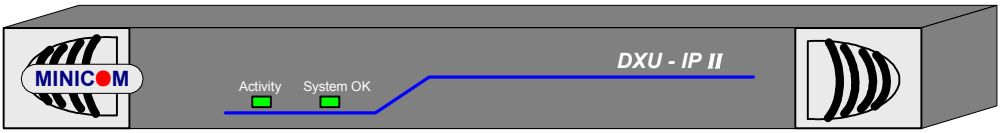

Figure 2 Front panel

The table below explains the functions of the front panel LEDs.

LED	Function
Activity	LED solid when a remote user operates the DXU IP II
System OK	LED solid when DX User IP II connected and functioning

5.1 DX User IP II rear panel

Figure 3 illustrates the rear panel of the DX User IP II.

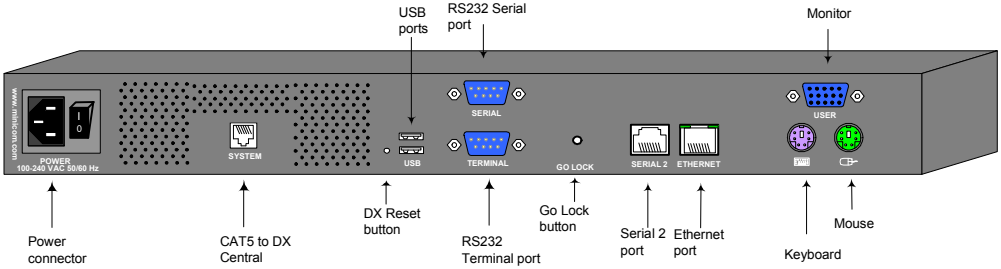

Figure 3 DX User IP II rear panel ports

DX Reset button

The DX Reset button resets the DX parts of the DX User IP II.

Go Lock button

The Go Lock button disconnects the active remote session and returns control to the local user.

Serial / Serial 2 port

The Serial port is only used for KVM.net managed mode when the DX User IP II is the Master Console – see page 30.

In Standalone and KVM.net enable modes, the Serial 2 port can be used for any RS232 application, e.g. managing a router or power switch.

Terminal port

In Standalone and KVM.net enable modes only, when there are X-RICC RS232s in the DX system, you can control them through an RS232 terminal connected to the DX User IP II.

Ethernet - Connects the DX User IP II to an Ethernet network.

USB ports

Update the DX firmware via a Minicom Flash USB key. See the DX User Guide for information on updating firmware.

System port – Used to connect the DX User IP II to the DX Central.

KVM ports – Used for optional local console.

6. Rack mounting the DX User IP II

Use the L-shaped brackets and screws provided to mount the DX User IP II on a server rack as illustrated below.

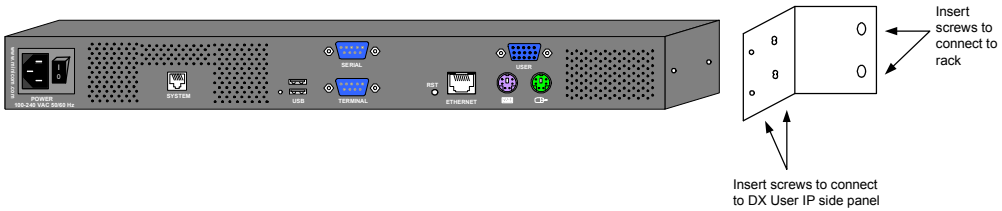

Figure 4 Connecting the L-shaped brackets

7. Pre-installation guidelines

- Place cables away from fluorescent lights, air conditioners, and machines that are likely to generate electrical noise
- The maximum distance between each device (computer, KVM switch or second level DX Central) and the DX Central is 100m/330ft. The maximum distance between the DX Central and the DX User IP II is also 100m/330ft. For best performance place the DXU IP II as close as possible to the DX Central.

8. Connecting the DX User IP II

Figure 5 below illustrates the connections of the DX User IP to the DX system. See below for more details.

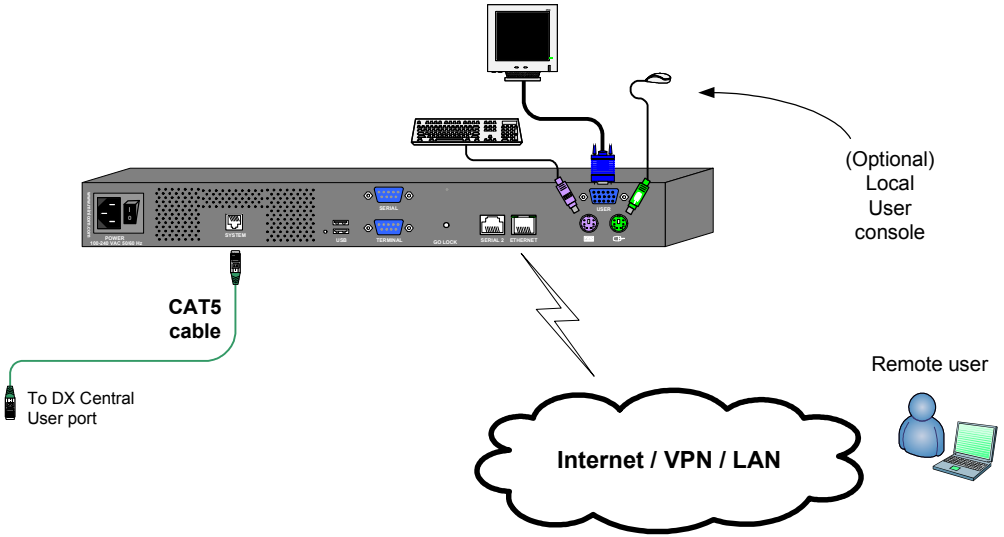

Figure 5 DX User IP connections

8.1 Connecting the DX User IP to the WAN/LAN

The Ethernet connector on the DX User IP II can be used either for a 100 Mbps 100BASE-TX connection or for a 10 Mbps 10BASE-T connection. The adapter adjusts to the appropriate operation mode automatically.

To connect to a LAN/WAN, connect an Ethernet cable to the DX User IP II Ethernet port and the Network switch.

8.2 Connecting the DX User IP II to the DX Central unit

For **KVM.net managed** mode connect a CAT5 cable to the DX User IP II System port and to DX Central User port 1. This DX User IP II must be assigned as the Master Console – see page 30. Where there are more than one IP devices in the DX system, (e.g. DX User IP II units or IP Access connected to a DX User unit etc), one of them must be connected to User port 1 of the DX Central. The others can be connected to any other User port number.

For **Standalone and KVM.net enabled** modes connect a CAT5 cable to the DX User IP II System port and to any DX Central User port.

8.3 Local User

To use the DX User IP II locally, connect a keyboard, video and mouse, as illustrated in Figure 5.

8.4 Serial cable - KVM.net managed mode only

The Serial cable is only used when this DX User IP II is assigned to be the Master Console in KVM.net managed mode – see page 30. Note! The Master Console IP device must be connected to User Port 1 of the DX Central unit.

Connect the Serial cable as illustrated below.

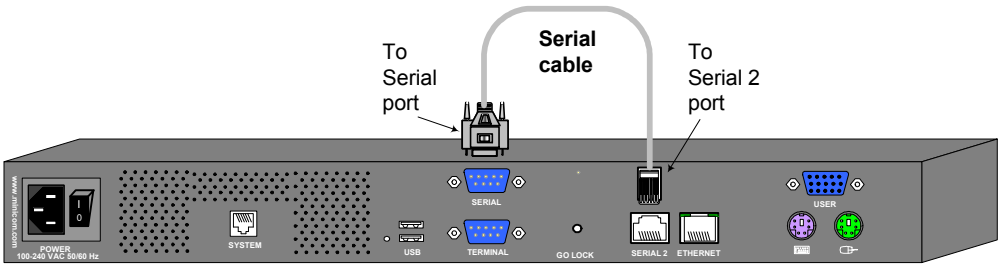

Figure 6 Serial cable

8.5 Connecting an RS232 terminal

Connect the RS232 terminal to the DX User as illustrated in the figures below.

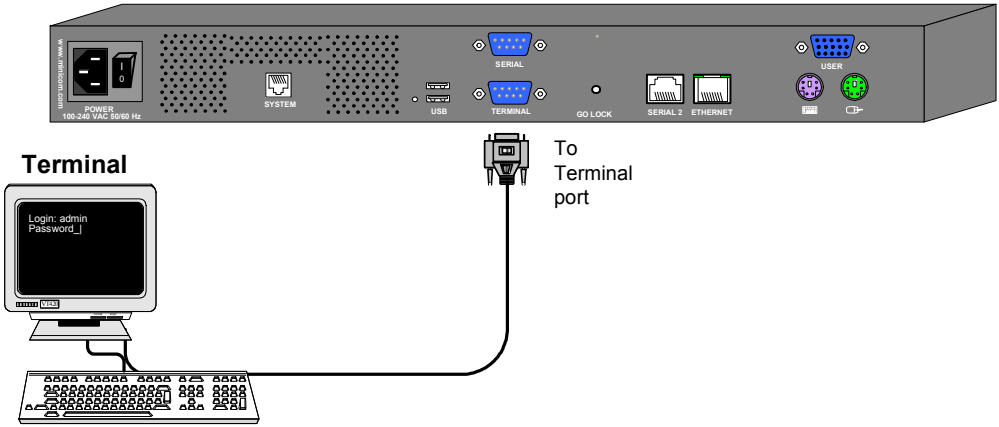

Figure 7 Connecting the RS232 terminal

8.5.1 Order of powering on

Connect the DX User IP to the power supply using the power cord provided.

The devices and servers can be powered on at any time. Power on the DX components in the following order:

1. The primary and secondary level DX Centrals.
2. The DX User and DX User IP II units.

9. Configuring the system – web interface

How to configure the system depends on how the DX User IP II is being used. There are 3 possible options - Standalone, KVM.net enabled or KVM.net managed. The sections below explain how to configure the system for each mode. Sections that deal with some and not all modes are clearly marked.

9.1 Initial settings - Default IP address

By default, DXU IP II boots with an automatically assigned IP address from a DHCP (Dynamic Host Configuration Protocol) server on the network. The DHCP server provides a valid IP address, gateway address and subnet mask.

To identify the IP address, the DXU IP II MAC address appears on the underside of the DXU IP II box. The device number (D.N.) can also be found there.

If no DHCP server is found on the network, DXU IP II boots with the static IP address:192.168.0.155.

Note! If a DHCP server later becomes available, the unit picks up the IP settings from DHCP server. To keep the static IP address, disable DHCP – explained in section 10.1 on page 13.

9.2 Static IP addresses for a number of units

Where you want to connect more than 1 DXU IP II to the same network and there is no DHCP server, or you want to use static IP addresses, do the following:

Connect the DXU IP II units one at a time and change the static IP address of each unit before connecting the next unit.

9.3 Logging into the Web interface

Complete the initial setup via the Web configuration interface:

1. Open your Web browser (Internet Explorer version 6.0 or higher).
2. Type the DXU IP II system IP address - https://*IP address*/config - and press **Enter**. The login page appears, see Figure 8.

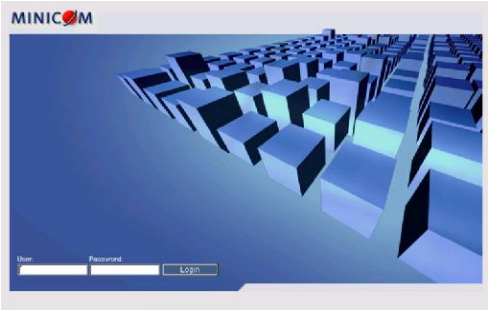

Figure 8 Login page

3. Type the default Administrator user name **- admin -** and password **- access -** (both lower case).
4. Press **Enter**. The Web interface opens at the Network Configuration page. See Figure 9.

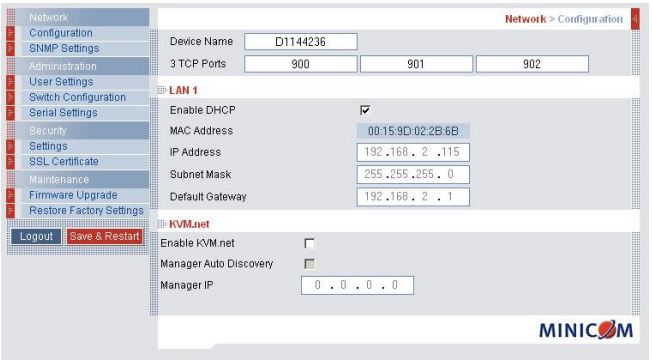

Figure 9 DXU IP II Web interface

5. Bookmark the page for easy reference.

9.4 SSL Certificate notes

When first connecting to DXU IP II's https configuration page, 2 browser security warnings appear. Click **Yes** to proceed.

The first warning disappears upon first DXU IP II client installation, when Minicom's root certificate is installed.

10. Network > Configuration

Consult your Network Administrator for the network settings.

Device name - Type a name for the DXU IP II. Default device name consists of the letter 'D' followed by the 6-digit device number (D.N.) found on the silver label on the underside of the DXU IP II box.

3 TCP Ports - Choose any 3 TCP ports from port #800 to 65535. (When managed by KVM.net® II, the port numbers can be changed from KVM.net interface if needed).

Note

Firewall or router security access list must enable inbound communication through the selected TCP ports for the DXU IP II's IP address.

For Client computer access from a secured LAN, the selected ports should be open for outbound communication.

10.1 LAN 1

Under LAN 1 in Figure 9, is the following:

Enable DHCP – When a DHCP server is active on the same network to which DXU IP II is connected, DHCP provides automatic IP assignment.

When DHCP is disabled – (Recommended) – You can assign a fixed IP address to the DXU IP II.

Consult your Network Administrator regarding the use of the DHCP. **Note!** Where you have access to the server – your configured (or default) DXU IP II device name will appear on the DHCP server's interface, making it easy to locate.

When DHCP is disabled, enter the **IP Address, Subnet Mask,** and **Default Gateway** for **LAN 1**, as given by your Network Administrator.

10.2 KVM.net

Standalone mode – The **Enable KVM.net** box must be unselected. Go straight to section 11 Administration > User Settings.

KVM.net enabled/managed - The Enable KVM.net must be selected to allow DXU IP II unit to be remotely managed by Minicom's KVM.net system.

Manager Auto Discovery – when checked, KVM.net automatically detects the DXU IP II, if it resides on the same network segment.

Manager IP – If DXU IP II resides on a different segment, type the static IP address of the KVM.net Manager. (We advise typing the static IP address of the KVM.net Manager even if the DXU IP II resides on the same network segment as the KVM.net Manager).

For KVM.net enabled/managed go straight to section 19 Saving changes, on page 23. Once the DXU IP II is KVM.net enabled, all device configuration settings are done via the KVM.net interface.

11. Administration > User Settings

Note! This section is only relevant to Standalone mode.

From the menu click **User Settings**, Figure 10 appears.

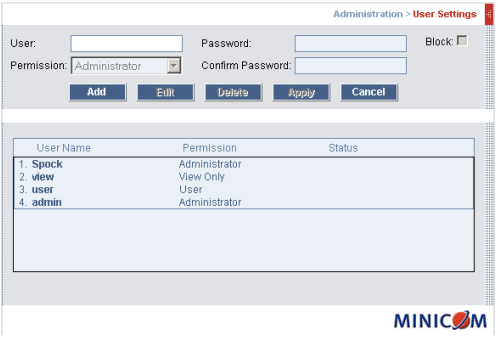

Figure 10 User Settings

Although there are Users in the DX system created in the AIM interface, these can only access the system locally. To access the system over IP, you must create Users in the web interface.

On this page an Administrator creates and edits users.

There are 3 levels of user access:

- Administrator
- User
- View only

Administrator
An Administrator has unrestricted access to all windows and settings and can "take over" any active session (explained in section 22.2 on page 34). An Administrator can change the name and password of all users, change the network settings and assign names to Targets servers.

User
A User can access/control Target Servers, but cannot use the advanced mouse settings. A User has no access to the Web configuration interface.

View only
View only can view the screen of the currently accessed Target Server without keyboard and mouse control. A "view only" indicator appears on the viewer's local mouse pointer.

11.1 Adding a user

To add a user:

1. Click Add and type a name and a password. The password must be at least 6 characters – letters or numbers, and must not include the user name, even if other characters are added.

   Note! The following "special" characters: &, <, >, ", {, } cannot be used for either the user name or password.

   Depending on the security level chosen the user name and password parameters are different. See section 14 on page 18.

2. Select the permission type from the **Permission** box.
3. Click Apply, the user appears in the list of users.

11.2 Editing a user

To edit a user:

1. Select the user from the list.
2. Click Edit. You can now change all the parameters – user name, permission and password.
3. Click Apply, the changes are saved.

11.3 Deleting a user

To delete a user:

1. Select the user from the list.
2. Click Delete.
3. Click Apply, the changes are saved.

11.4 Blocking a user

An alternative to deleting a user is blocking a user. This means that the user's name and password is stored, but the user is unable to access the system. Check **Block** to block a user. Uncheck **Block** to allow the user access.

12. Administration > Switch Configuration

Note! This section is only relevant to Standalone mode.

1. From the menu click **Switch Configuration**. The Switch Configuration window appears, see Figure 11.

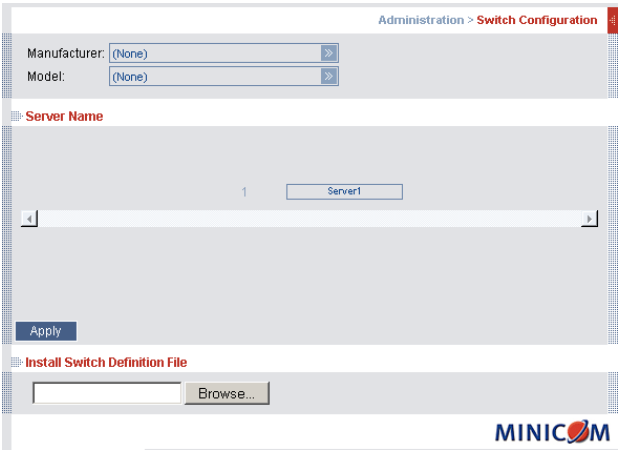

Figure 11 Switch Configuration

2. From the **Manufacturer** drop-down list select Minicom.
3. From the **Model** drop-down list select the DX system according to the number of Central units in the system – 32 ports for 1 Central unit, 64 ports for 2 Central units etc. The number of possible connected servers appears in the **Server Name** section.
4. In the **Server Name** section, change the name of the connected servers by selecting the server name and typing a new name. **Note!** Match the server names here to the server names in they appear in the DX AIM.
5. Click Apply to save changes.

Install switch definition file

In the event that Minicom's Technical Support updates the Switch Definition file, the file will be available in the Support section of our website - www.minicom.com.

1. Download the file onto the Client computer and unzip it to a temporary folder.
2. Locate and install the Switch Definition file. The switch definition file is replaced.

13. Administration > Serial Settings

Note! This section is only relevant to Standalone mode.

Where you have a Serial device connected to the DXU IP II you must configure the RS232 settings.

To do so:

From the menu click **Serial Settings**, the **Serial Settings** appear, see Figure 12.

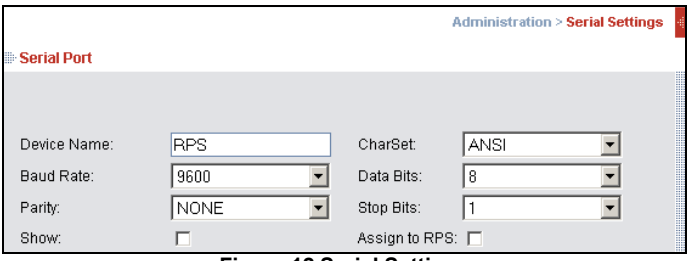

Figure 12 Serial Settings

Type a device name and choose the correct device parameters. Note! Where you have a Minicom Serial Remote Power Switch connected, see below **Assign to RPS**.

13.1 Show

Tick **Show** to make the Serial device appear in the list of servers/devices that can be accessed during a remote session.

13.2 Assign to RPS

Where a Minicom Serial Remote Power Switch (RPS) is connected to the Serial port, tick this box. All other parameters are then grayed out. See the RPS Installation Guide for further information on installing and operating the RPS.

14. Security > Settings

Note! This section is only relevant to Standalone mode.

Configure the security features, such as Account Blocking, Password Policy and Idle Timeout, as explained below.

From the **Security** section click **Settings**, the **Security Settings** appear, see Figure 13.

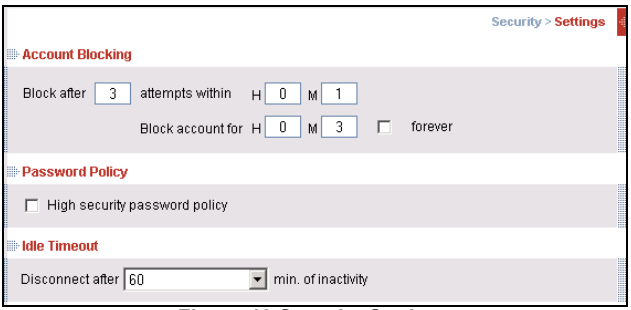
Security > Settings
Account Blocking
Block after 3 attempts within H 0 M 1
Block account for H 0 M 3 forever
Password Policy
High security password policy
Idle Timeout
Disconnect after 60 min. of inactivity

Figure 13 Security Settings

The Security Settings fields:

Account Blocking – decide on the number of attempts to login with a wrong username or password after which there is a time lock or a total block.

Password Policy – You have the option of a standard or high security level of password. The table below shows the parameters of the 2 options.

Standard security policy	High security policy
6 characters or more	8 characters or more must include at least 1 digit and 1 upper case letter and 1 “special” character as follows !@#$%^*()_-+=[]’:;?/
Must not include the user name	Must not include the user name

Check the box to enable the high security password policy. Unchecked, the standard security policy applies.

Idle Timeout – Select the Timeout inactivity period after which the user is disconnected from the system. Choose **No Timeout** to disable Timeout.

15. Security > SSL Certificate

Note! This section is only relevant to Standalone mode.

You can install an SSL certificate.

To do so:

From the menu, select **SSL Certificate**, the install SSL Certificate page appears, see Figure 14.

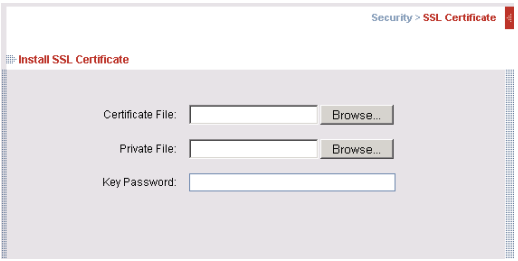

Figure 14 Install SSL Certificate page

Certificate File - Browse to locate the **cer** file.

Private File - Browse to locate the **private key** file.

Key Password - Type the "private key" password.

16. Maintenance > Firmware Upgrade

Note! This section is only relevant to Standalone mode.

Upgrade the DXU IP II firmware to take advantage of new features. Download the firmware from the Support section of Minicom's website –www.minicom.com. Save the firmware file on the Client computer.

From the menu select **Firmware Upgrade**. The Firmware Upgrade window appears showing the current firmware version see Figure 15.

Figure 15 Firmware Upgrade

1. Locate and upload the firmware file.
2. Verify the current and uploaded version of the firmware.
3. Click Start Upgrade. The upgrade starts. On completion, click Reboot. The unit reboots. After about 30 seconds the Login page appears.

Note!

Depending on the type of firmware upgrade, the following settings may be erased: User settings, server names, mouse and video adjustments. For more information refer to the firmware release notes.

The network settings remain intact.

17. Restore Factory Settings

You can restore the DXU IP II unit to the factory settings. This restores the original DXU IP II parameters, resetting all the information added by the administrators, including: Network settings*, Servers, Switches, Users, Passwords etc.

* You have the option to preserve Network settings – explained below.

Warning! Once reset the data cannot be retrieved.

To restore factory settings:

1. From the menu select **Restore Factory Settings**. Restore Factory Settings appears see Figure 16.

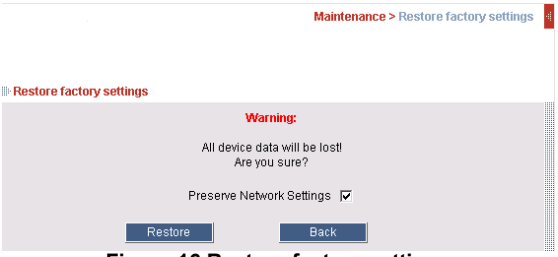

Figure 16 Restore factory settings

2. Check the box if you want to preserve Network settings.
3. Click Restore.

18. Troubleshooting - Safe mode

From the Safe mode you can:

Restore factory defaults - When you cannot access the system e.g. you have forgotten the Username or Password, restore factory defaults from the Safe mode. (Section 17 on page 20 explained how to restore factory settings from the Web interface).

Restore the device firmware – If during a firmware update there is a power failure and you can no longer access the system you can restore the device firmware from the Safe mode.

18.1 Entering Safe mode

To enter Safe mode:

1. Press and hold down the **Go Lock** button for 3-4 seconds and at the same time power up the DXU IP II. The device boots up in Safe mode.
2. Wait until the unit finishes booting (1-2 minutes).
3. You need to know the IP address of the DXU IP II. The IP address depends on whether there is a DHCP server on the network. If there is, the DHCP server assigns an IP address to the DXU IP II. If there is no DHCP server, the unit boots with the static IP address 192.168.2.155.

   Open Internet Explorer and type the following into the Address box: http://*IP address*/config. (Do not start the address with **https**). The Login page appears, see Figure 17.

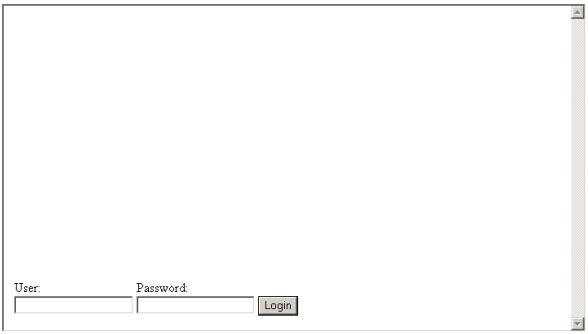

Figure 17 Login page

4. Type username: **admin** , password: **SAFEmode**. (Case sensitive). (This username and password works only in Safe mode). A menu appears, see Figure 18.

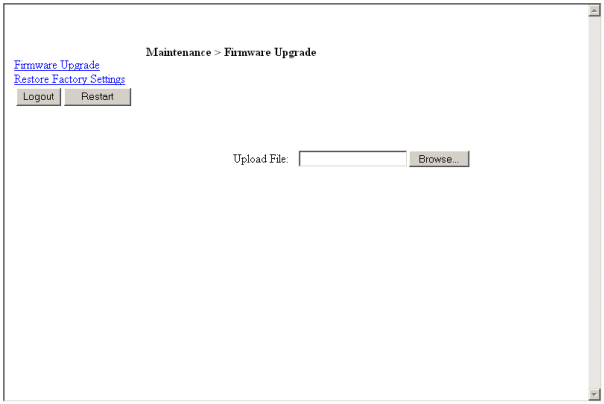

Figure 18 Safe mode menu

18.2 Restoring factory defaults

To restore factory defaults:

1. From the menu choose **Restore Factory Settings**. A warning appears see Figure 19.

Figure 19 Warning

2. Click Restore. A further warning appears, see below.

Figure 20 Warning

3. Click OK, the factory defaults are restored. When the process finishes Figure 21 appears.

Figure 21 Reboot

4. Click **Reboot** to restart the unit.

18.3 Restoring the device firmware

Contact Minicom Technical Support support@minicom.com, to receive the Safe Mode Upgrade firmware required to restore the device firmware. Save the firmware file on the hard disk of a computer connected to the network.

To restore the device firmware:

1. From the Safe mode menu choose Firmware Upgrade.
2. Locate the firmware file and click Install, then click Start Upgrade. The firmware upgrades.When the process finishes Figure 22 appears.

Figure 22 Reboot

3. Click **Reboot** to restart the unit.

19. Saving changes

Click Save & Restart to save configuration changes and restart the DXU IP II.

Only one Administrator can log into the Configuration area at a time. An idle timeout of 30 minutes terminates the session.

For Standalone and KVM.net enabled and managed modes the DX AIM needs to be configured, see the next section.

20. Configuring the DX AIM

Configuration of the DX system depends on how the DX User IP II is being used - Standalone or KVM.net managed. The sections below explain how to configure the system for each mode.

1. From a remote computer console open Internet Explorer (6.0 and above) and type the DXU IP II's IP address. https://*IP address*. (Note! Only SSL connections are allowed, therefore type HTTPS before the IP address or the name of the DXU IP II). The DX Login page appears, see Figure 23.

Or at the DXU IP II local console once the system is connected and powered on the DX Login page appears, see Figure 23.

Figure 23 DX Login page

2. Type the username and password and press Enter. By default, the user name is: **admin** and the password is **admin**, (both lower case).

On connection, the DX AIM appears, see Figure 24. Figure 24 shows the Servers page already configured with a number of servers.

If the DX system has never been configured, the Servers page appears blank. To configure/manage the DX system, see the DX User Guide.

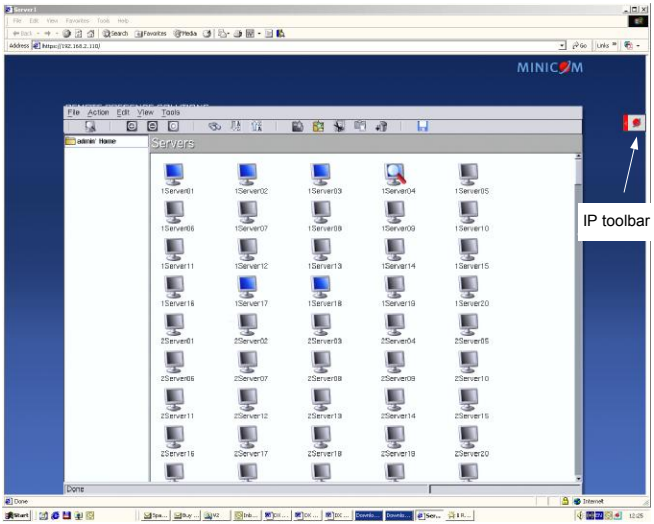

Figure 24 Servers page

20.1 Standalone and KVM.net Enabled modes - DX AIM configuration

For KVM.net managed mode, go to section 20.2.

From the Tools menu click Settings, the Settings window appears. See Figure 25.

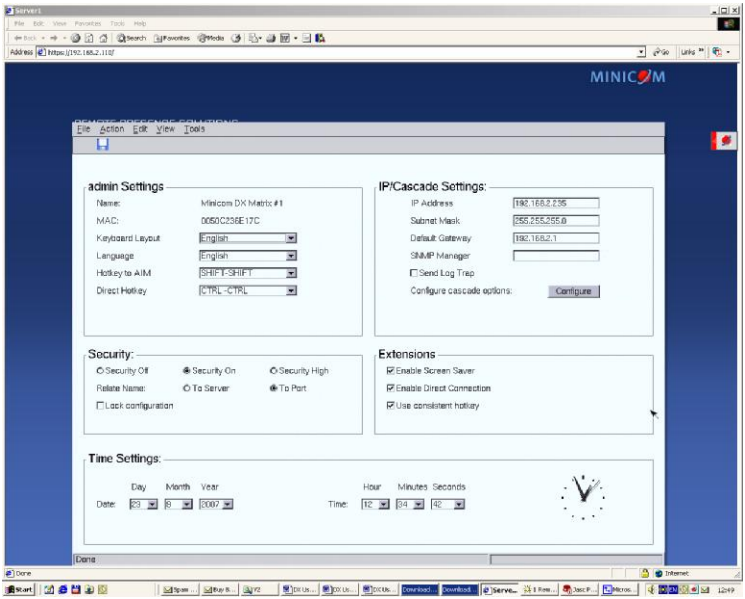

Figure 25 Settings window

In Settings, ensure that **Direct Hotkey** is set to CTRL-CTRL (default).

In Extensions, select **Enable Direct Connection** and **Use consistent hotkey**.

To save changes click File/Save changes, or .

20.2 KVM.net managed mode - DX AIM configuration

If the DXU IP II is being used as a Master Console, ensure the Serial cable is connected to the DX User IP II, see page 9. Also ensure the DX User IP II is connected to the DX Central User port 1.

1. From the View menu choose DX System Configuration. The DX System Configuration window appears. See Figure 26.

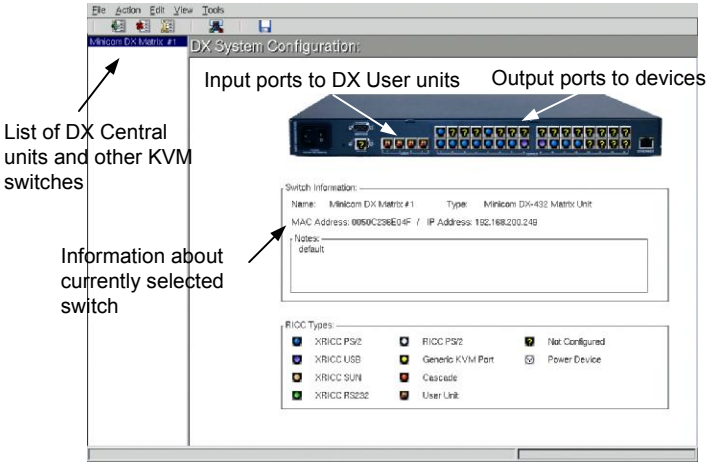

Figure 26 DX System Configuration window

The above figure shows the rear ports of a DX Central unit, including the DX User units.

2. Click a DX User unit. The Configuration box appears, see Figure 27.

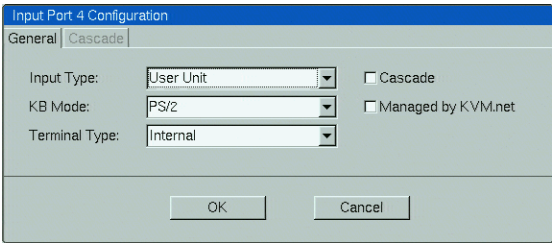

Figure 27 Configuration box

3. Select the Managed by KVM.net checkbox.
4. Click OK.

Once a DX User unit is KVM.net managed:

- You loose local KVM access from this unit
- X-RICC RS232 units cannot be connected to the DX system

5. Repeat steps 2-4 for all DX User IP II units.
6. Save the settings and manually restart the DX User IP II units. The DX User IP II is now fully managed by the KVM.net system.

20.2.1 Accessing AIM when the DX system is KVM.net managed

When the DX is KVM.net managed when attempting to access the AIM interface, it does not appear. Instead the screen appears black with a message stating that the DX system is KVM.net managed.

To access the AIM (to e.g. disable the KVM.net managed mode):

1. From a remote computer console type the DXU IP II's IP address. You connect to one of the servers in the DX system.
2. Press left **Shift**, **Shift**. The screen appears black, with the KVM.net managed message.
3. Press Ctrl, Esc, A – press each key one after the other, not all together. The AIM appears. You can now make the desired adjustments.

21. Configuring the KVM.net

Configuration for KVM.net enabled/managed modes is done in the KVM.net Manager GUI. The sections below explain the KVM.net configuration steps specifically related to the DXU IP II.

See the KVM.net User Guide to set up and manage the KVM.net system.

1. Open the KVM.net GUI and from the menu select Settings/KVM Switches, the KVM Switches page appears, see Figure 28.

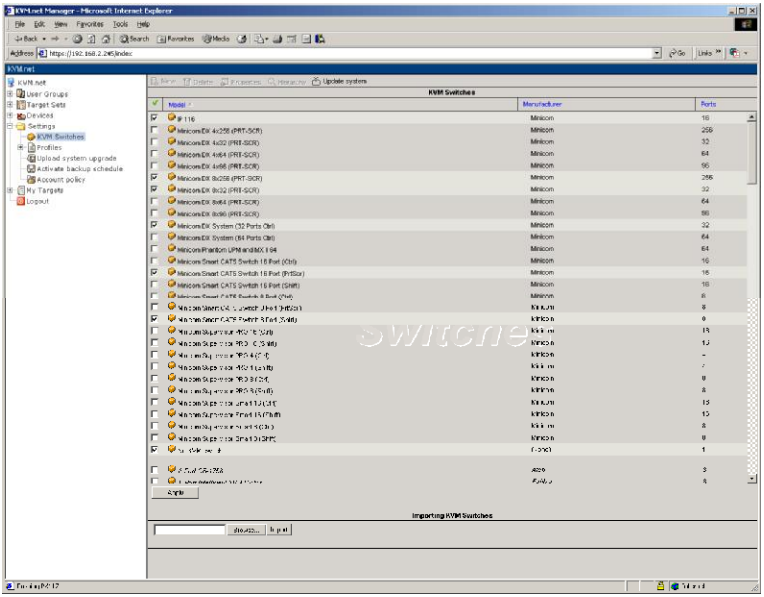

Figure 28 KVM Switches page

2. For **KVM.net enabled** select the correct DX configuration with Ctrl (and not PRT-SCR hotkey). For example when there is 1 DX Central unit in the DX system, select **Minicom DX System (32 ports Ctrl)**. When there are 2 DX Central units in the DX system select **Minicom DX System (64 ports Ctrl)**.

   For **KVM.net managed** select the correct DX configuration with PRT-SCR (and not Ctrl hotkey). For example when there is 1 DX 432 Central unit in the DX system, select **Minicom DX 4 x 32 (PRT-SCR)**. When there are 2 832 DX Central units in the DX system select **Minicom DX 8 x 64 (PRT-SCR)**.

3. From the menu select Devices, the Devices page appears, see Figure 29.

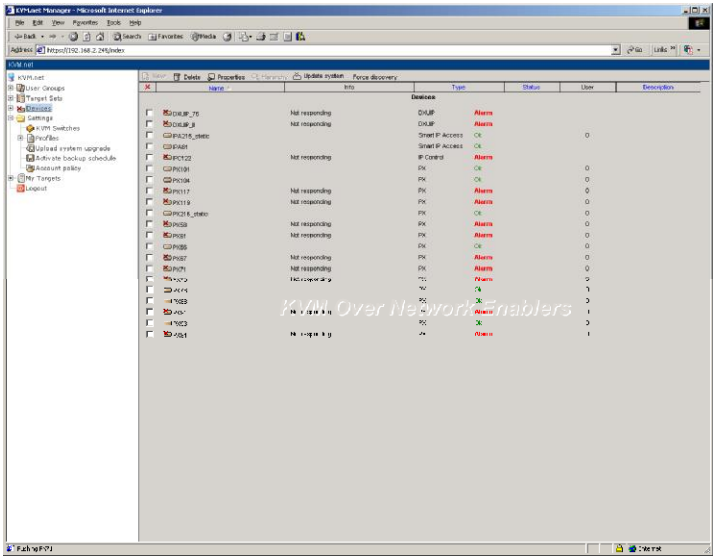

Figure 29 Devices page

4. Double-click the DXU IP II device. The Device Properties General tab appears, see Figure 30.

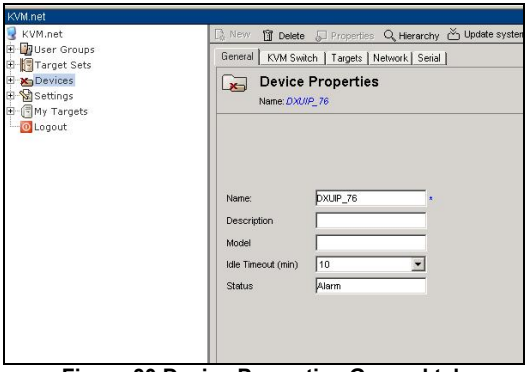

Figure 30 Device Properties General tab

5. In the name field give the device a unique name.
6. Click the KVM Switch tab, the following appears.

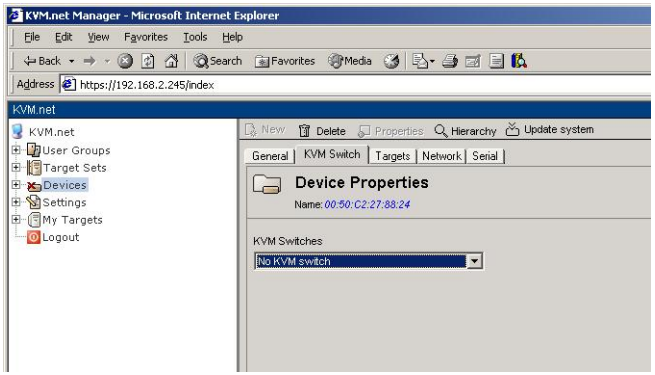

Figure 31 KVM Switch tab

7. In the KVM Switches field select as follows:

   For **KVM.net enabled** select the correct DX configuration with Ctrl (and not PRT-SCR hotkey), as selected in the KVM Switches page see page 28 above.

   For **KVM.net managed** select the correct DX configuration with PRT-SCR (and not Ctrl hotkey), as selected in the KVM Switches page see page 28 above. Once the correct DX configuration with PRT-SCR is selected, the KVM Switch tab appears as in Figure 32.

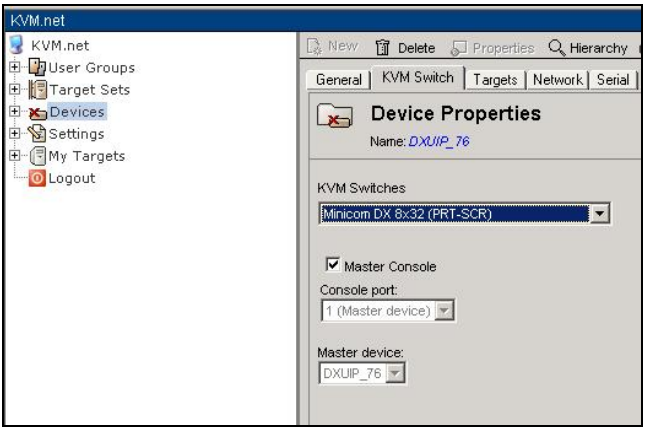

Figure 32 KVM Switch tab of DXUIP II in KVM.net Managed mode

Master Console – **KVM.net managed only.** If this DX User IP II is the IP device connected to User port 1 of the DX Central, select the Master Console checkbox. (This enables the DX port statuses to be displayed in the KVM.net interface). If this unit is not the master console, select the User port this device is connected to from the Console port drop-down menu and select the Master Device from the Master device drop down menu.

21.1 Connecting more than one DXU IP II to the system

When there are more than one DXU IP II units in the system you must do the following:

1. Select the KVM switch file for all DXU IP II units. So follow steps 3 – 7 above for each DXU IP II unit.
2. In Device Properties click the Targets tab, see Figure 33. Here you assign the Target servers to the specific ports of the DXU IP II unit. You must assign the same Targets to the same ports for each DXU IP II unit.
3. Assign the ports for one DXU IP II unit
4. Go to the Devices page and select the next DXU IP II unit,
5. Click the Targets tab and in the Targets drop-down menu select All Targets
6. Go down the list and again assign the same Target servers to the same ports for this DXU IP II unit.

   When selecting a port the KVM.net checks which DXU IP II unit is available and automatically connects you to the chosen Target. If a local DX User is accessing the port View Only is available.

For all other configuration settings see the KVM.net User Guide.

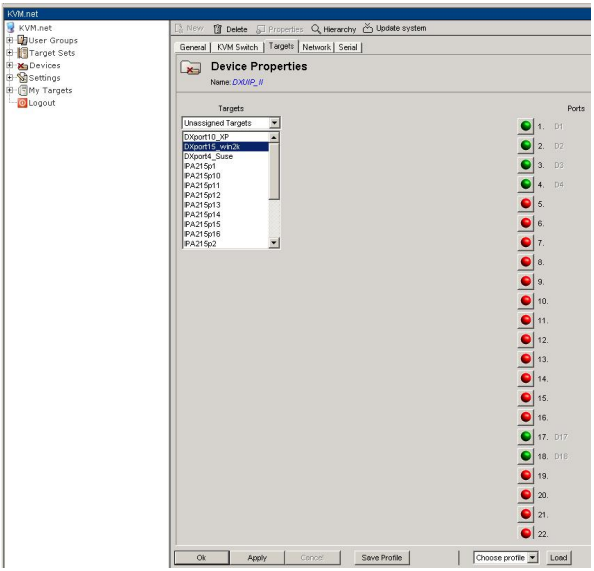

Figure 33 Targets tab

22. Operating the system

How to operate the system depends on how the DX User IP II is being used – Standalone, KVM.net enabled or KVM.net managed.

- For Standalone, operation is only via the IP toolbar
- For KVM.net enabled, operation is via the IP toolbar or KVM.net Manager
- For KVM.net managed, operation is via the IP toolbar or KVM.net Manager

The sections below explain how to operate the system for each mode.

22.1 Accessing servers/devices via the IP toolbar

In Standalone mode - From a remote computer console open Internet Explorer (6.0 and above) and type the DXU IP II's IP address. https://*IP address*. The DX Login page appears, see Figure 23. Type the username and password and press Enter. The DX AIM appears, see Figure 24. Login to AIM and use the IP toolbar for switching between the servers.

When access is via IP, you should not switch to the servers/devices using the DX AIM, but only via the IP toolbar, see Figure 24.

In KVM.net Enabled and Managed modes, - First login to the KVM.net and then select the server you want to access in All My Targets list. If the system is working in KVM.net Enabled mode, the AIM login will appear. Login to the AIM and then select the required server from the IP toolbar again. Switch between the servers using the IP toolbar or KVM.net Manager.

The IP Toolbar features are now explained.

22.1.1 The IP Toolbar

To maximize the Toolbar:

Click the arrow . Click again to minimize the Toolbar.

The Toolbar can be dragged and dropped to anywhere on the screen, by clicking and dragging the logo .

To hide the Toolbar, either:

Double-click the Smart IP Access System tray Icon .

Or press **F9**.

To display the Toolbar repeat the above actions. See also page 43.

22.1.2 Accessing a server/device

To connect to a server/device:

Important!

Accessing or switching to the servers from the IP toolbar only works when the DX AIM is on the Servers/Devices page, see Figure 24.

1. Select **View/Servers/Devices** to display the Servers/Devices page.
2. From the Toolbar, click , or right-click . A list of connected servers/devices the user has permission to access appears. **Note!** These are the server names as configured in the IP interface and not the DX AIM interface – we recommend giving the servers the same names in both the IP and DX portions.
3. Click the desired server or Serial device. The screen of the server or the Serial device window appears. See Figure 34.
4. To switch to a different server repeat steps 1 and 2 above.
5. To display the DX AIM press the left **Shift** key twice.
6. On logging out and then logging in again, the screen of the last accessed server/device appears.

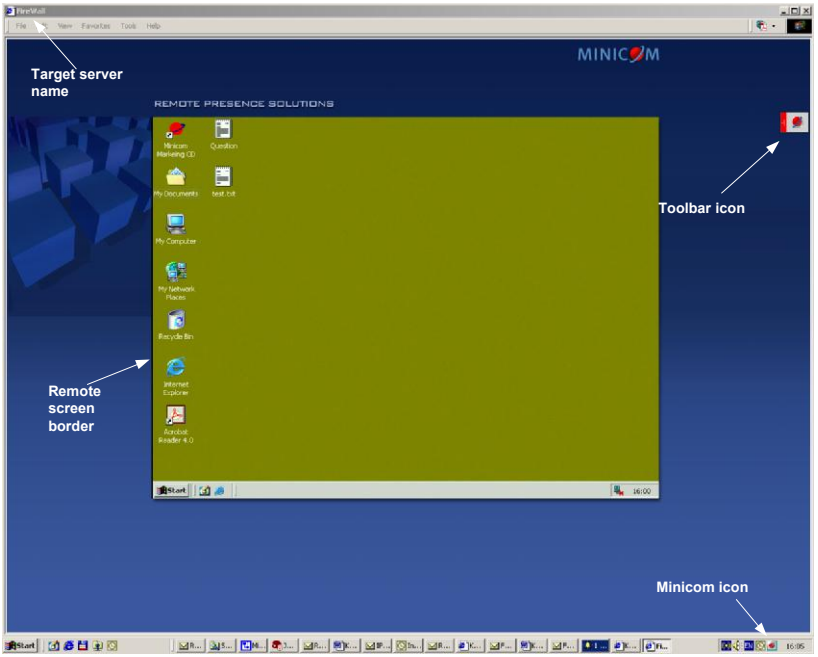

Figure 34 Remote console window

On the remote console you have the following:

Target server name - The currently accessed server identity can be checked by looking at the Server name on the Internet Explorer title bar.

Toolbar icon – This is the minimized toolbar from which you switch and configure the system.

Minicom icon – Hold the mouse over the icon to view information about current server, connection time and video mode.

22.2 Taking over a busy remote session

While only one user can have control, many users can be connected simultaneously. When connecting to a busy Target Server an Administrator has the option to take over the Target Server. A User only has this option when the current session is run by another User, but not by an Administrator. The following message appears

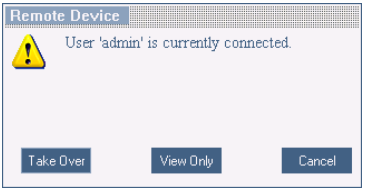

Figure 35 Busy remote session options

Choose to Take Over or View Only or Cancel.

When watching a screen in View Only mode you can Double click inside the Remote screen border – see Figure 23 – to take over the remote control. The current user sees a message stating that control has been taken over.

22.3 Full screen mode

Work on the Target Server as if you are working on a local computer, with full screen mode.

To work in full screen mode:

1. Ensure that the Client computer has the same screen resolution as the Target Server.
2. Press **F11**. The Internet Explorer window disappears, leaving the Internet Explorer menu bar at the top.
3. Right click the Internet Explorer menu bar and check Auto-Hide. The Internet Explorer menu bar disappears. You are in full screen mode.

To exit full screen mode:

Press **F11**. Or place the mouse at the top of the window to display the Internet Explorer toolbar and click the Restore button.

Note! Full screen mode can also be activated from the Toolbar menu, see page 43.

22.4 Changing the performance settings

You can alter the bandwidth settings from the Toolbar.

To alter the settings:

From the Toolbar, click . The Settings.. box appears, see Figure 36.

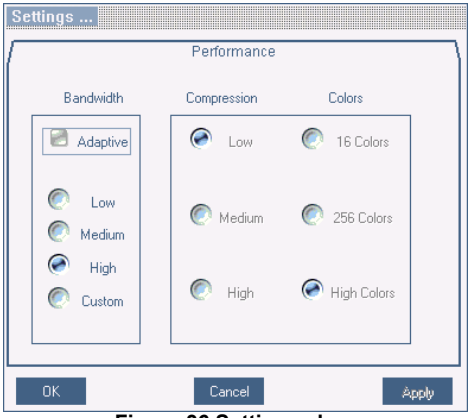

Figure 36 Settings.. box

Bandwidth

Choose from the following options:

Adaptive – automatically adapts to the best compression and colors.

Low - Select Low for high compression and 16 colors.

Medium - Select medium for medium compression and 256 colors. Medium is recommended when using a standard internet connection.

High - For optimal performance when working on a LAN, select High. This gives a low compression and high colors (16bit).

Custom – You can choose your own compression and color levels.

Click **OK**. The screen of the last accessed Target Server appears.

22.5 Adjusting the Video settings

To change the video settings:

From the Toolbar, click . You have the following options:

- Refresh
- Manual Video Adjust
- Auto Video Adjust

Each option is explained below.

22.5.1 Refresh

Select Refresh or press **Ctrl+R** to refresh the Video image. Refresh may be needed when changing the display attributes of a Target Server.

22.5.2 Manual Video Adjust

Use the manual video adjustment for fine-tuning the Target Server video settings after auto adjustment or for adapting to a noisy environment or a non-standard VGA signal or when in full-screen DOS/CLI mode.

To adjust the video manually:

1. Click Manual Video Adjust. A slider bar appears. See Figure 37. Also a red frame appears around the screen. This represents the screen area according to the Server's screen resolution. Perform the adjustments inside and relative to this frame.

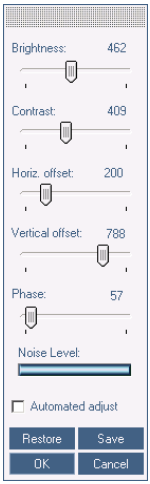

Figure 37 Manual Video Adjustments controls

2. Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.

Brightness / Contrast - use the scales to adjust the brightness and contrast of the displayed image.

Horizontal Offset - defines the starting position of each line on the displayed image.

Vertical Offset - defines the vertical starting position of the displayed image.

Phase - defines the point at which each pixel is sampled.

Noise Level - represents the Video "noise" when a static screen is displayed.

Automated adjust – When checked, the video adjusts automatically whenever there is a change in the screen resolution.

22.5.3 Auto Video Adjust

To adjust the video automatically:

We recommend opening Windows Explorer (or similar) in the background.

Click **Auto Video Adjust**. The process takes a few seconds. If the process runs for more than 3 times, there is an abnormal noise level. Check the video cable and verify that no dynamic video application is running on the Target Server's desktop.

Perform the procedure where necessary for each Target Server or new screen resolution.

22.6 Power cycle

Only in Standalone and KVM.net enabled modes

Where a Minicom Remote Power switch is connected to the Serial port of the DX User IP II, you can power manage the Target servers as follows:

From the Toolbar, click . The Power menu appears, see below.

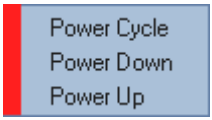

Figure 38 Power menu

To send a power cycle command or to power down or up the currently accessed Target server, select the appropriate option.

Note! Only the currently accessed Target server is affected, so to power manage other Target servers you must access each one individually.

22.7 Keyboard key sequences

Click . A list of defined keyboard sequences appears. When clicked, these transmit directly to the Target Server, and will not affect the Client computer.

For example, select **Ctrl-Alt-Del** to send this three key sequence to the Target Server to initiate its Shutdown/Login process.

To add a keyboard sequence:

Click **Add/Remove**. The Special Key Manager box appears see Figure 39.

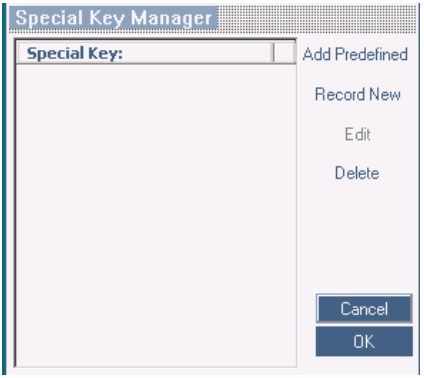

Figure 39 Special Key Manager box

To add a predefined sequence:

1. Click Add Predefined. A list of sequences appears.
2. Select the desired sequence and click OK. The sequence appears in the Special Key Manager box.
3. Click OK. The sequence appears in the Keyboard Key sequence list.

To record a key sequence:

1. From the Special Key Manager box press **Record New**. The Add Special Key box appears see Figure 40.

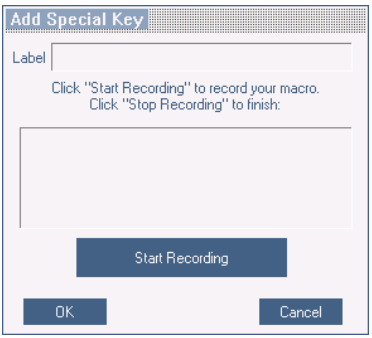

Figure 40 Add Special Key box

2. Give the key sequence a name in the Label box.
3. Click **Start Recording**.
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

To edit a key sequence:

1. From the Special Key Manager box select the desired key.
2. Click **Edit**.
3. Click **Start Recording**
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

22.8 Synchronizing mouse pointers

When working at the Client computer, two mouse pointers appear: The Client computer's is on top of the Target Server's. The mouse pointers should be synchronized. The following explains what to do if they are not synchronized.

Warning

Before synchronizing mouse pointers adjust the video of the Target Server, (explained above) otherwise mouse synchronization may not work..

22.8.1 Aligning the mouse pointers

When accessing the Target Server, the mice may appear at a distance to each other.

To align the mouse pointers:

From the Toolbar click / **Align** or press **Ctrl+M** simultaneously. The mice align.

22.8.2 Calibrating mouse pointers

A Target Server may have a different mouse pointer speed to the Client computer. Calibrating automatically discovers the mouse speed of the Target Server and aligns the two pointers.

To perform the calibration when the Target Server Operating system is, Windows NT4, 2000 or 98:

From the Toolbar click / **Calibrate**. Smart IP Access saves this alignment so calibration is only needed once per Target Server.

If the Video Noise Level is above zero, calibration may not work. Go to Video Adjustment and try to eliminate the noise by pressing Auto video adjust and/or adjusting the bars in Manual video adjust, then perform the mouse calibration.

Note! If the mouse settings on the Target Server were ever changed, you must synchronize mouse pointers manually, as explained below.

22.8.3 Manual mice synchronization

Only in Standalone mode. (For KVM.net enabled and managed modes, the mouse settings are done in the KVM.net Manager web interface.)

If the mouse settings on the Target Server were ever changed, or when the Operating system on the Target Server is, Windows XP / 2003 Server / Vista, Linux, Novell, SCO UNIX or SUN Solaris you must synchronize the mouse pointers manually.

To manually synchronize mouse pointers:

1. From the Toolbar click / **Manual Settings**. The **Mouse Settings** box appears see Figure 41.

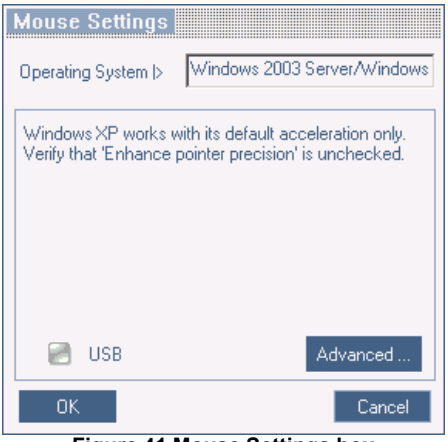

Figure 41 Mouse Settings box

2. Select the Target Server's Operating System and click OK. Instructions and sliders appear.
3. Follow the instructions and set any relevant sliders to the same values as set in the Target Server's Mouse Properties window.

2 examples!

For Windows XP, go to the Mouse settings on the Target Server and uncheck Enhance pointer precision.

For Windows NT4. If Mouse Properties were ever changed for the Target Server – even if they have been returned to their original state - uncheck default - Default.

Click **OK**. The mouse pointers should be synchronized.

USB

The USB option in Mouse Settings box is available for X-RICC USB and for unsupported operating systems and SUN Solaris. Use this option if you are sure of the custom acceleration algorithm you are using, or have been informed so by customer support.

Advanced – Mouse Emulation

In the Advanced Mouse settings, you can set the type of mouse that you would like DXU IP II to emulate. We recommend not changing the advanced settings unless there is erratic mouse behavior (the mouse is making random clicks and jumping arbitrarily around the screen).

Click Advanced ... the Mouse Emulation box appears see Figure 42.

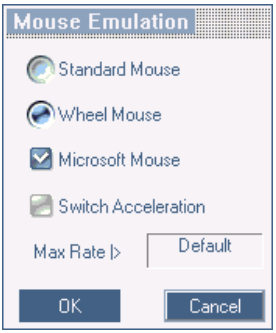

Figure 42 Mouse Emulation box

Select the mouse connected to the Local Console port on the DXU IP II, e.g. if the local mouse is a non-Microsoft 2 button mouse, select **Standard Mouse** and uncheck **Microsoft Mouse**.

Max Rate - this defines the maximum mouse report rate. For Sun Solaris the default value is 20 in order to support older Sun versions.

22.9 Minicom logo menu features

Right click the Minicom logo , a menu appears. From this menu you can access the connected devices. You also have the following features:

Disconnect – You can disconnect the session by clicking Disconnect.

About - Click About to verify the Client, Firmware, KME (Keyboard/Mouse Emulation firmware) and Switch file versions installed on your DXU IP II.

Local Settings – Click Local settings, the Client Configuration box appears, see Figure 43.

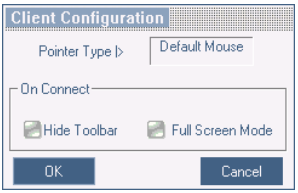

Figure 43 Client Configuration box

Pointer type – From the Drop-down menu you can change the Client computer mouse pointer to appear as a dot or to not appear at all.

Hide Toolbar – Check this option to hide the Toolbar from the next reconnection onwards. To toggle the Toolbar on and off, press **F9**. See above page 32.

Full Screen Mode - Check this option to make the remote session screen appear in full screen mode from the next reconnection onwards. To toggle the full screen mode on and off, press **F11**.

22.10 Disconnecting the remote session

To disconnect the remote session:

On the Toolbar, click .

For **KVM.net managed** mode the User disconnects from the server and from the remote session.

For **Standalone and KVM.net enabled** modes the User disconnects from the server and from the remote session. The DXU IP II remains logged into the AIM.

You can download and install an SDF (RPC extension file), which when clicking will disconnect from the Server, the remote IP session and the DX AIM. So to re-login, for Standalone and KVM.net Enabled modes, you need to login to the DXU IP II web interface and then to DX AIM again. In KVM.net Managed mode the DXU IP II remains in Managed mode. Contact Minicom Support at support@minicom.com for more information.

22.11 Accessing servers/devices via KVM.net

Note! This section is relevant to KVM.net enabled and managed modes.

From the KVM.net GUI, Targets are accessed from the My Targets folder. See the KVM.net User Guide for further details. Note! Only permitted Targets appear in the list.

23. Video resolution and refresh rates

The DX User IP II supports the following video modes. Do not use other custom video settings.

Hz →	56	60	65	66	70	72	73	75	76	85	86
640x480		x		x	x	x		x		x	
720x400					x					x	
800x600	x	x				x		x		x	x
1024x768		x			x	x	x	x	x	x	
1152x864								x			
1152x900				x					x		
1280x720		x									
1280x768		x						x			
1280x960		x								x	
1280x1024		x				x		x	x	x	
1600x1200		x	X		x			x		x	

24. Technical specifications

Operating systems	**Target Server** DOS, Windows, Novell, Linux, SUN Solaris Unix **Client Computer** Windows 2000 or higher with IE 6.0 or higher and Installation of signed ActiveX controls must be enabled in the Client computer.
Resolution	**Target Server** Up to 1600 x 1200 @ 85Hz **Client Computer** Recommended - resolution should be higher than on Target Server
Video and mouse synchronization	Both auto and manual modes
Security	128-bit SSL encryption
DX User IP II to local KVM connection	Screen – HDD15; Keyboard/Mouse – MiniDIN6
LAN connection	RJ45 – LAN, Autosensing 10/100 Mbit/s
Serial connections	DB9 - RJ45
System connector to DX Central	RJ45
Cable types	CAT5, CAT6, CAT7
Dimensions	43.2x27x4cm / 17X11X1.6”
Power supply	100 – 240 VAC 50 / 60 Hz
Operating temperature	0°C to 40°C / 32° to 104°F
Storage temperature	-40°C to 70°C / -40° to 158°F
Operating humidity	10% to 90% (non-condensing)
Storage humidity	5% to 95% (non-condensing)
Warranty	3 years

25. Safety

The device must only be opened by an authorized Minicom technician. Disconnect device from AC mains before service operation!

26. User Guide feedback

Your feedback is very important to help us improve our documentation. Please email any comments to: ug.comments@minicom.com

Please include the following information: Guide name, part number and version number (as appears on the front cover).

27. WEEE compliance

WEEE Information for Minicom Customers and Recyclers

Under the Waste Electrical and Electronic Equipment (WEEE) Directive and implementing regulations, when customers buy new electrical and electronic equipment from Minicom they are entitled to:

- Send old equipment for recycling on a one-for-one, like-for-like basis (this varies depending on the country)
- Send the new equipment back for recycling when this ultimately becomes waste

Instructions to both customers and recyclers/treatment facilities wishing to obtain disassembly information are provided in our website www.minicom.com.